Remarks

The election is affirmed.

The indicated allowability of Claims 7, 9, 12-16, 18, 20, 27, 29, 32-35, 38, 40, 47, 49, 52-55, 58-60, 68, 70, 73-75, 80, 82, and 85-87 is gratefully acknowledged.

The amendments herein, it is believed, cure the claim misnumbering objections and the indefiniteness rejection of Claim 41. Also, two of the elected independent claims (65 and 77) have been amended as set forth further below to recite subject matter that has been held to be allowable, leaving at issue only the substantive rejections of the remaining elected claims as being obvious over Srivastava (USPN 6,684,331) in view of Aiello et al. (USPN 6,397,329), with the rejections of Claims 21 and 22 additionally relying on Van Rijnsoever et al. (USPP 2002/0090090) and with the rejections of Claims 17, 36, 37, 56, 57, 76, and 88 adding in "official notice".

As admitted in the Office Action, Srivastava fails to teach partitioning users who are not in a revoked set into disjoint subsets having associated subset keys, with Aiello et al. being used to show users partitioned into subsets on the ground that the proposed combination would provide Srivastava "a less expensive public key revocation system".

The rejection is deficient for two reasons. First, the proposed combination of references would not arrive at Claim 1, because in Aiello et al. the relied-upon partitioning shown in Figures 6a and 6b is to update certificates, not keys, col. 10, lines 19-55. The certificates in Aiello et al. appear to be used for conventional certificate uses, namely, verifying a user's identity. They are certainly not used to encrypt any session keys as recited in independent Claims 1 and 61.

Accordingly, combining Aiello et al. with Srivastava would not arrive at Claim 1. Instead, Srivastava's system would be modified to update certificates as taught by Aiello et al., but since these certificates are nowhere taught in Aiello et al. as private encryptors, much less encryptors of session keys, the relied-upon group key of Srivistava would still be encrypted using the individual user private keys as taught by Srivistava.

The second deficiency in the rejection is that while the object of Aiello et al. indeed is to provide a less expensive public key revocation system, this does not suffice as a fair prior art suggestion to combine Aiello et al. with Srivistava, because Srivistava does not indicate that its system suffers from any particular expense problems, and Aiello et al. does not suggest that systems such as Srivistava's are overly expensive. Thus, the proferred motivation is at best a motivation to use Aiello et al. in a vacuum, but not in the context of Srivistava, thereby failing to meet the requirements of MPEP §2143.

With respect to independent Claim 21 (and Claim 41 as well), neither Srivistava nor Aiello et al. nor Van Rijnsoever et al. teach or suggest "stateless" receivers. Furthermore, the key in Van Rijnsoever et al. is transmitted in an ECM which, per the relied-upon paragraph [0017], is itself a message in a packet stream, not necessarily a header. Indeed, Van Rijnsoever et al. nowhere mentions the word "header", a rather peculiar omission of a well-known term of art in a technical reference if indeed the reference contemplated using a "header".

With respect to the rejection of Claims 17, 36, 37, 56, 57, 76, and 88 on the basis of "official notice", a prior art showing in support of the examiner's position is hereby seasonably requested under MPEP §2144.03 should this rejection be persisted in. Note that Claim 17 does not recite "PN generator" in a vacuum, but rather using a PN generator to assign labels to subsets, and evaluating the pseudorandom

sequence generator during decryption. Accordingly, even if a PN generator is found, absent a prior art suggestion to combine it with other references to arrive at the particular invention set forth in Claim 17, the claim is patentable.

Independent Claim 65 has been amended to recite the limitations of allowable (and now-canceled) Claim 68.

Allowable Claims 70 and 73-75 have been rewritten in independent form albeit without incorporating any claims that might have formerly intervened between them and the underlying independent claim.

Independent Claim 77 has been amended to recite the limitations of allowable (and now-canceled) Claim 82.

It appears that the non-elected but still pending claims are patentable as well, and their reinstatement and allowance is earnestly solicited.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

Respectfully submitted,

John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1053-121.AMD